

✓ FILED _____ ENTERED
_____ LOGGED _____ RECEIVED

4:25 pm, Nov 19 2020

AT BALTIMORE
CLERK, U.S. DISTRICT COURT
DISTRICT OF MARYLAND
BY _____ Deputy

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

IN THE MATTER OF THE SEARCH OF
FOUR CELLULAR PHONES
CURRENTLY LOCATED AT 31
HOPKINS PLAZA, BALTIMORE,
MARYLAND

Case No. 1:20-mj-2803 TMD

**AFFIDAVIT IN SUPPORT OF
APPLICATION FOR SEARCH WARRANT**

I, Special Agent Christian Aanonsen, with the Bureau of Alcohol, Tobacco, Firearms, and Explosives (“ATF”), being first duly sworn, hereby depose and state as follows:

I. PURPOSE OF THIS AFFIDAVIT

1. I submit this affidavit in support of an application for a search warrant authorizing the search of the following cellular telephones, as described in more detail in Attachment A, and are all in custody at the ATF Baltimore Field Office, located at 31 Hopkins Plaza, Baltimore, Maryland:

- a. Samsung Galaxy S9, bearing IMEI 356917091573886 (**SUBJECT DEVICE 1**);
- b. Samsung Galaxy A10, bearing IMEI 353290112938774 (**SUBJECT DEVICE 2**);
- c. Samsung A20, bearing IMEI 355369104338892 (**SUBJECT DEVICE 3**); and,
- d. REVVL 2 Plus, bearing IMEI 015248000070993 (**SUBJECT DEVICE 4**);

collectively, the “**SUBJECT DEVICES**”.

2. Based on the facts set forth in this affidavit, I submit there is probable cause to believe that Kevin VICE possessed a firearm as a prohibited person in violation of 18 U.S.C. § 922(g), and is involved in drug distribution and conspiracy to do so, in violation of 21 U.S.C. §§ 841, 846. The search warrant would authorize members of the ATF, or their authorized representatives including other law enforcement agents assisting in the above described

investigation, to examine the **SUBJECT DEVICES** for the purpose of seizing electronically stored data described in Attachment B.

II. AFFIANT BACKGROUND AND EXPERTISE

3. I am a Special Agent with the ATF and currently assigned to a joint task force comprised of ATF agents and detectives from the Baltimore City Police Department (“BPD”). In my capacity as a Special Agent, I am “an investigative or law enforcement officer” of the United States within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Section 2516 of Title 18, United States Code.

4. I have been employed by the ATF since 2014 and successfully completed the Criminal Investigator Training Program and Special Agent Basic Training Academies at the Federal Law Enforcement Training Center located in Glynco, Georgia. Prior to joining the ATF, I was a police officer for the Department of Defense for two years. I hold a Bachelor’s Degree in Law and Justice Studies from Rowan University in Glassboro, New Jersey.

5. I have been the case agent in complex multi-defendant, multi-jurisdictional criminal organization cases. I have participated in multiple Title III wiretap investigations as a case agent, monitor and member of surveillance teams. I have conducted covert surveillance of suspected controlled dangerous substance (“CDS”) traffickers and interviewed individuals involved in the CDS trafficking trade. Based on my training and experience, I am familiar with the manner in which CDS is transported, stored and distributed, the methods of payment for such CDS, and the manner in which CDS traffickers communicate with each other.

6. Through my training and experience, I know the habits, methods, routines, practices, and procedures commonly employed by persons engaged in trafficking firearms and

their unlawful possession. Traffickers use cellphones to coordinate with suppliers, customers, and co-conspirators. They frequently switch phones or use multiple phones to evade detection. I also know the techniques employed by traffickers to keep records of their trafficking activities, to conceal proceeds of their illegal conduct, and to evade law enforcement. For example, they use cellphones, addresses, and vehicles subscribed or registered to names other than their own in order to avoid detection by law enforcement.

7. I also know that persons prohibited from possessing firearms will often utilize unlawful means of obtaining them such as burglaries and theft and trading them for narcotics. Information surrounding the unlawful transfer of firearms and their prohibited possession is often memorialized within the possessor's cell phone. Cell phones may also contain images of the firearms with or without their possessor and communication documenting their transfer.

8. Further, individuals involved with illegal activities tend to use their cellular devices to call or text accomplices after the crime has been committed. Additionally, an individual may communicate with another person to strategize and attempt to hide the belongings or merchandise from the crime committed. More specifically, I know that members of criminal activities use cellular telephones to further their objectives by:

- a. Communicating with other co-conspirators by talking and by sending email messages, text messages, and messages through social media (e.g., Facebook);
- b. Storing contact information of co-conspirators; and
- c. Taking photographs and recording videos of co-conspirators and contraband.

9. I am aware that drug trafficking is an ongoing and recurring criminal activity. As contrasted with crimes against persons, which tend to be discrete offenses, drug trafficking is an illegal commercial activity that is characterized by regular, repeated criminal activity.

10. Cellular telephones are an indispensable tool of the narcotics trafficking trade. Narcotic traffickers use cellular telephones, push-to-talk telephones, Short Message Service (“SMS”), electronic-mail, and similar electronic means and/or devices, often under fictitious names or names other than their own, in order to maintain contact with other conspirators and narcotic traffickers. In addition, narcotic traffickers will often change their cellphones following the arrest of a member of their Drug Trafficking Organization (“DTO”), or at random in order to frustrate law enforcement efforts.

11. Drug traffickers keep and maintain records of their various activities. Such records are regularly concealed in a suspect’s automobile, residence, office, and on his person, and that they take various forms. Documents commonly concealed by traffickers, include but are not limited to notes in code, deposit slips, wired money transactions, hidden bank accounts, photographs of co-conspirators, various forms of commercial paper, personal address books, notebooks, records, receipts, ledgers, travel receipts (rental receipts, airline tickets, bus tickets, and/or train tickets) both commercial and private, money orders and other papers relating to the ordering, transportation, sale and distribution of controlled dangerous substances or other such documents which will contain identifying data on the co-conspirators. These items are kept in locations that are considered safe by the drug traffickers such as safety deposit boxes, residences, vehicles and on their person, where they have ready access to them.

12. Drug traffickers use cellular telephones, pagers and other electronic communications devices to facilitate illegal drug transactions. The electronically stored information on these devices is of evidentiary value in identifying other members of the drug trafficking conspiracy and establishing the relationship between these individuals, including photographs and other identifying information stored on these devices;

13. Drug traffickers use computers or other electronic storage media, including smart phones, to store the records documents, or items listed in paragraphs 11 and 12 above.

14. I submit this affidavit for the limited purpose of establishing probable cause for a search warrant. I have not included every fact known to me concerning this investigation to date. Rather, I set forth only those facts I believe are necessary to establish probable cause. I have not, however, excluded any information known to me that would defeat a determination of probable cause. The information set forth in this affidavit derives from my personal knowledge and observations; discussions with other ATF agents and law enforcement officers, and witnesses; and my review of police reports and public records. All conversations and statements described in this affidavit are related in substance and in part unless otherwise indicated.

III. PROBABLE CAUSE

15. On May 21, 2020, at approximately 3:30 p.m., BPD officers were operating a marked police vehicle in the 4500 block of Saint Georges Avenue in Baltimore City. Officers observed a Lexus bearing Maryland Registration 3EC1254 parked the wrong way opposing the flow of traffic. The Lexus was running and had tint so dark that officers could not see through it. Officers made contact with the driver, Kevin VICE, who was sitting alone in the driver's seat. As officers were speaking to VICE they detected the odor of marijuana emanating from the vehicle, and observed, in plain view, an open container of an alcoholic beverage in the center console cup holder.

16. Officers asked VICE if there was anything else inside the vehicle and he stated there was some marijuana in the car. Officers had VICE exit the Lexus. Officers conducted a search of the vehicle and located in the center console was a Taurus Model 850 revolver. The firearm was loaded with five .38 caliber cartridges. The firearm was not secured in any way and

was within close proximity to VICE in the vehicle.

17. Officers also recovered \$7,310 from the center console, and three plastic bags of suspected marijuana, a schedule I controlled substance. When officers questioned VICE about the currency, he knew the exact amount that was in the vehicle. Additionally, the vehicle was registered to VICE.

18. Officers recovered the **SUBJECT DEVICES** from the front driver's compartment area near the center console.

19. All recovered evidence, including the firearm, was submitted to the Evidence Control Unit of BPD.

20. After his arrest, VICE was held without bail and made a series of recorded jail calls. On May 22, 2020, at 5:49 p.m., VICE told an unknown male ("UM") that, "A lot of people owe up but I can't get to them because of my phone." This call occurred the day after his arrest and subsequent seizure of the **SUBJECT DEVICES**. I know based on my training and experience that drug traffickers will keep "owe" sheets in which they document who owes them money for narcotics they have provided. These "owe" sheets can also be stored on cell phones.

21. Prior to the events set forth in this affidavit, VICE was convicted in 2010 of possession with intent to manufacture and distribute a controlled dangerous substance in the Circuit Court for Baltimore City. He was sentenced to 15 years of incarceration, with 14 years and 8 months suspended, and supervised probation for 3 years. Given this sentence, VICE is prohibited from possessing a firearm and should be aware that he had been convicted of a crime that carries a punishment of over a year in prison. Further, at the time of his arrest he told officers that he was a "felon," after being advised of his rights pursuant to *Miranda*.

22. The firearm was test-fired at the BPD Firearms lab and expelled a projectile by the

action of an explosive, and therefore qualifies as a firearm under 18 U.S.C. § 921(a)(3). The firearm was not manufactured in Maryland and therefore affected interstate commerce

23. Since VICE's arrest, he has not had access to the **SUBJECT DEVICES** in order to destroy, delete, or otherwise tamper with any data on the **SUBJECT DEVICES**. For this reason, I believe any data and information contained on the **SUBJECT DEVICES** generated by VICE, may be recovered by a forensic analysis.

IV. BACKGROUND CONCERNING ELECTRONIC COMMUNICATIONS DEVICES

24. The fruits and instrumentalities of criminal activity are often concealed in digital form. Furthermore, digital camera technology is often used to capture images of tools and instrumentalities of pending criminal activity. The **SUBJECT DEVICES** have both digital storage capacity and digital camera capabilities.

25. Individuals who possess firearms as prohibited persons in violation of 18 U.S.C. § 922(g) and are involved in drug trafficking offenses in violation of 21 U.S.C. § 841 and 846, often use cell phones to communicate with suppliers, to place orders with suppliers, to communicate with customers, to receive orders from customers, and to arrange meeting times and locations for the distribution of controlled substances. The individuals engaging in drug trafficking will often use a combination of voice calls and text messages to coordinate drug transactions. Individuals engaged in drug trafficking offenses also use digital storage devices to maintain telephone number "contact lists" of individuals who may have assisted in the planning of this and other criminal activity.

26. Narcotic traffickers often place nominal control and ownership of telephones in names other than their own to avoid detection of those telephones by government agencies. Even

though telephones are in the names of other people, drug traffickers retain actual ownership, control, and use of the telephone, exercising dominion and control over them.

27. Drug traffickers utilize different types of communication devices, and change the numbers to these communication devices frequently. This is done to avoid detection by law enforcement personnel. Also, as noted above, drug traffickers dedicate different communication devices for different aspects of the trafficking organization.

28. Cellular phones associated with drug traffickers include various types of evidence. Phones may contain relevant text messages or other electronic communications; they may contain electronic address books listing the phone numbers and other contact information associated with co-conspirators; and they may contain other types of information.

29. Prohibited persons and drug traffickers often take photos of themselves with firearms, large quantities of controlled substances, money, or high-end consumer items, like cars or watches. These “trophy” photos are often maintained on cellular telephones to be shared on social media, or as symbols of their success.

30. Finally, the mere fact of a cellular phone’s call number, electronic serial number or other identifying information may be of evidentiary value as it may confirm that a particular cell phone is the phone identified during a wiretap, pen register, or other electronic investigation.

V. FORENSIC ANALYSIS OF ELECTRONIC COMMUNICATIONS DEVICES

31. Based on my training and experience, I know that electronic devices such as cellular phones (smartphones) can store information for long periods of time. Similarly, things that have been viewed via the internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools. There is probable cause to believe that things that were once stored on the **SUBJECT DEVICES** may still be stored on those devices,

for various reasons, as discussed in the following paragraphs.

32. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the **SUBJECT DEVICES** were used, the purpose of its use, who used it, and when.

33. There is probable cause to believe that this forensic electronic evidence might be on the **SUBJECT DEVICES** because data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

34. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

35. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

36. The process of identifying the exact electronically stored information on a storage

medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

37. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

38. Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premise. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

39. During this case and in numerous others involving complex DTOs, investigators have learned that the drug-trafficking organization relies heavily on electronic devices to facilitate drug trafficking. It is necessary to conduct a physical inspection of the electronic devices in order to obtain electronic communications and other information that might be stored on the seized phones and to determine whether any of the seized phones were the subject of wiretap, pen register or other investigation detailed herein. The phones may also contain data and communications that were not electronically intercepted due to encryption or for other reasons.

40. Again, the **SUBJECT DEVICES** remain in the custody of law enforcement. The only known specifics of each phone requested for authorization to search are detailed in Attachment A and the types of information expected to be recovered from the devices are listed in

Attachment B.

VI. CONCLUSION

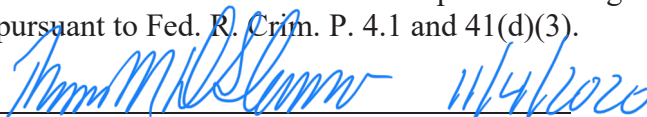
41. Accordingly, there is probable cause to believe that evidence will be found from an analysis of the recovered **SUBJECT DEVICES**. The **SUBJECT DEVICES** may contain the records of the most recent calls, which may include calls with persons involved in the offense(s). The **SUBJECT DEVICES** may contain copies of SMS or text or other electronic communications relating to activities associated with the offense(s). The **SUBJECT DEVICES** may also contain a variety of other electronic evidence, including electronic communications through various cellular or internet-based applications, photographs and other information.

42. Wherefore, in consideration of the facts presented, I respectfully request that this Court issue a search warrant for the **SUBJECT DEVICES**, and authorize the search of the items described in Attachment A, for the information set forth in Attachment B, where applicable, which constitute fruits, evidence and instrumentalities of possessing a firearm as a prohibited person, in violation of 18 U.S.C. § 922g, and drug distribution and conspiracy in violation of 21 U.S.C. §§ 841, 846.

Respectfully submitted,
CHRISTIAN AANONSEN
Digitally signed by CHRISTIAN
AANONSEN
Date: 2020.11.03 10:58:16 -05'00'

Special Agent Christian Aanonsen
Bureau of Alcohol, Tobacco, Firearms, and Explosives

Sworn to before me over the telephone and signed by me
pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3).


The Honorable Thomas DiGirolamo
United States Magistrate Judge

ATTACHMENT A
Items to be Searched

The **SUBJECT DEVICES**,

- a. Samsung Galaxy S9, bearing IMEI 356917091573886 (**SUBJECT DEVICE 1**);
- b. Samsung Galaxy A10, bearing IMEI 353290112938774 (**SUBJECT DEVICE 2**);
- c. Samsung A20, bearing IMEI 355369104338892 (**SUBJECT DEVICE 3**); and,
- d. REVVL 2 Plus, bearing IMEI 015248000070993 (**SUBJECT DEVICE 4**),

were all recovered from VICE on May 21, 2020, and are currently in custody of the ATF Baltimore Field Division, located at 31 Hopkins Plaza, Baltimore, Maryland.

ATTACHMENT B**Items to be Seized**

All records contained in the items described in Attachment A, which constitute evidence of violations of 18 U.S.C. §§ 922(g) (prohibited person in possession of a firearm) and 21 U.S.C. §§ 841, 846 (drug distribution, and conspiracy to commit drug distribution) including the following items, as outlined below:

1. Contact logs that refer or relate to the user of any and all numbers on the Subject Electronic Devices.
2. Call logs reflecting date and time of received calls.
3. Any and all digital images and videos of persons associated with this investigation.
4. Text messages to and from the **SUBJECT DEVICES** that refer or relate to the crimes under investigation.
5. Records of incoming and outgoing voice communications that refer or relate to the crimes under investigation.
6. Voicemails that refer or relate to the crimes under investigation.
7. Voice recordings that refer or relate to the crimes under investigation.
8. Any data reflecting the phone's location.
9. Contact lists.
10. Any and all records related to the location of the user(s) of the devices.
11. For the **SUBJECT DEVICES**:
 - a. Evidence of who used, owned, or controlled the devices at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

- b. evidence of software that would allow others to control the Devices, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence of the attachment to the **SUBJECT DEVICES** of other storage devices or similar containers for electronic evidence;
- e. evidence of counter forensic programs (and associated data) that are designed to eliminate data from the Devices;
- f. evidence of the times the **SUBJECT DEVICES** were used;
- g. passwords, encryption keys, and other access devices that may be necessary to access the **SUBJECT DEVICES**;
- h. documentation and manuals that may be necessary to access the Devices or to conduct a forensic examination of the **SUBJECT DEVICES**;
- i. contextual information necessary to understand the evidence described in this attachment.

With respect to the search of any of the items described above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment (including CDs, DVDs, thumb drives, flash drives, hard disk drives, or removable digital storage media, software or memory in any form), the search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein, while permitting government examination of all the data necessary to determine whether that data falls within the items to be seized):

- 1. surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);
- 2. “opening” or cursorily reading the first few “pages” of such files in order to determine their precise contents;
- 3. “scanning” storage areas to discover and possibly recover recently deleted files;
- 4. “scanning” storage areas for deliberately hidden files; or

5. performing key word searches or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

If after performing these procedures, the directories, files or storage areas do not reveal evidence of the specified criminal activity, the further search of that particular directory, file or storage area, shall cease.

With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable. If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.